Bundeskriminalamt

**Tatort Internet –**
**eine globale Herausforderung für die Innere Sicherheit**

BKA-Herbsttagung vom 20. – 22. November 2007

# Polizei in der digitalen Welt

Vortrag

**Jörg Ziercke**

Präsident,

Bundeskriminalamt Wiesbaden

BKA

## AUSWIRKUNGEN DER TECHNOLOGISCHEN ENTWICKLUNGEN AUF KRIMINALITÄT UND KRIMINALITÄTSBEKÄMPFUNG

Meine sehr verehrten Damen und Herren,
zur Polizeiarbeit in der digitalen Welt möchte ich mit folgenden Thesen beginnen:

1. Globalisierung und Internationalisierung von Terrorismus und Organisierter Kriminalität lassen die Strafrechtspflege und Gefahrenabwehr an ihre territorialen und funktionalen Grenzen stoßen.
2. Technische Innovationssprünge prägen die Kriminalität des 21. Jahrhunderts. Die rasante Entwicklung der Informations- und Kommunikationstechnologie hat die weltweite Kommunikation, Interaktion und Datenspeicherung tiefgreifend gewandelt. Tat- und Tätertypologien verändern sich grundlegend.
3. Neuartige Kriminalitätsphänomene, u. a. Angriffe auf kritische Infrastrukturen über Bot-Netze, werden klassische Formen terroristischer Anschläge ergänzen. Die Verletzlichkeit moderner, vernetzter Infrastrukturen wird weltweit an Bedeutung gewinnen.
4. Kryptierung und Anonymisierung schaffen verfolgungsfreie Räume! Verschlüsselung verhindert den Zugriff auf Beweismittel, die auf digitaler Hardware abgelegt sind. Verschlüsselung verhindert den Zugriff auf Informationen und damit eine rechtzeitige Gefahrenabwehr.
5. Klassische hoheitliche Eingriffsinstrumente - wie die Wohnungsdurchsuchung oder die Beschlagnahme von Computern - reichen zur Bekämpfung terroristischer und organisierter krimineller Netzwerke nicht aus. Konspiration prägt das kriminelle Kommunikationsverhalten, religiös motivierter internationaler Terrorismus verfolgt seine Ziele weiterhin langfristig.
6. Der Verfassungswert einer wirksamen Strafverfolgung und Gefahrenabwehr erfordert die kontinuierliche Anpassung polizeilicher Instrumentarien. Wir müssen den von Terroristen und Schwerstkriminellen längst vollzogenen digitalen Quantensprung aufholen. Wer einer solchen Anpassung ausweicht, macht die Polizei nicht nur blind. Er kündigt auch das Sicherheitsversprechen des Staates gegenüber seinen Bürgern und damit die elementare Grundbedingung eines friedlichen Zusammenlebens auf.

Meine sehr verehrten Damen und Herren,
**wie hat sich die Ermittlungspraxis im digitalen Zeitalter bisher verändert?**

Durchsuchten Polizei und Staatsanwaltschaft vor fünf oder zehn Jahren die Wohnung eines Beschuldigten, ging es - neben den klassischen Tatmitteln - vor allem darum, schriftliche Unterlagen sicherzustellen:

- Handschriftliche Aufzeichnungen gaben Aufschluss über Tatvorbereitungen.
- Kontoauszüge und andere Bankunterlagen gaben Hinweise auf Kontobewegungen und Geldflüsse.
- Adressbücher gaben Aufschluss über Mittäter und andere Kontaktpersonen.
- Briefe dokumentierten die Korrespondenz der Täter.

Die Täter versteckten Unterlagen, die die Polizei nicht finden sollte, im Keller, in der Garage oder im Auto. Die Verschlüsselung von Nachrichten spielte - mit Ausnahme vom Linksextremismus und -terrorismus - keine Rolle.
Die Täter kommunizierten über Festnetzanschlüsse. Wollten sie sich konspirativ verhalten, wichen sie auf Telefonzellen aus.
Kriminaltechniker suchten auf Papier nach Finger- und DNA-Spuren. Handschriften- und Schreibmaschinen-Erkennungsdienst waren gefordert.

**Wie sieht die Situation heute aus?**

- Wir stoßen bei Durchsuchungen immer häufiger auf die unterschiedlichsten technischen Geräte: PCs, Notebooks, Handys, Digitalkameras, Spielkonsolen, Navigationsgeräte, MP3-Player - um nur einige potenzielle Beweismittel zu nennen.
- Computer mit einem Terabyte Festplattenspeicher sind keine Seltenheit mehr. Im Verfahren gegen die Anfang September in Oberschlehdorn festgenommenen jungen Männer werten wir derzeit 2,5 Terabyte an Daten aus. Ca. 300.000 Dateien sind zu prüfen. In anderen Ermittlungsverfahren sind die Datenmengen sogar noch größer.
- Die Täter legen längst nicht alle Informationen mit Beweiswert auf ihrem Computer ab - sondern stattdessen in den Weiten des Internets. Selten kommunizieren sie direkt per Mail. Terroristen werden in Ausbildungslagern im Umgang mit Laptops und konspirativer Kommunikation und Datenspeicherung geschult.
- Täter telefonieren heute - wenn überhaupt - fast ausschließlich über Mobilfunkgeräte. Die Überwachung von Festnetzanschlüssen hat bei der Terrorismusbekämpfung erheblich an Bedeutung verloren.
- Internetkriminelle können Tausende von Geschädigten mit einem Mausklick produzieren. Psychologische Hemmschwellen gibt es nicht mehr. Man muss sich nicht Auge in Auge gegenübertreten. Die Opfer bleiben anonym.
- Zunehmend kommunizieren die Täter über das Internet – nicht nur von zu Hause aus. Sie weichen stattdessen auf Call-Shops aus. Profis üben sich im Call-Shop-Hopping - 167 Anläufe in 33 Call-Shops im Falle der jüngst in Oberschlehdorn Verhafteten - oder nutzen offene WLAN-Zugänge unbeteiligter Dritter. Der WLAN-Technik scheint die Zukunft zu gehören.
- Die Verwendung von Breitbandanschlüssen ist mittlerweile die Regel. Mit einer Datentransferrate von bis zu 100 Megabits pro Sekunde ermöglichen Breitbandanschlüsse einen bis zu 2000mal schnelleren Internetzugang als analoge Anschlüsse. Die Folge: Die bei polizeilichen Maßnahmen auflaufenden Datenmengen sprengen die vorhandenen technischen Kapazitäten.
- Voice over IP, die Echtzeitübertragung von Sprache über das Internet, gewinnt weiter an Bedeutung. An die Stelle von leitungsvermittelten, monolithischen, nicht kryptierten Telefonaten über deutsche Anbieter treten zunehmend paketvermittelte, dislozierte, kryptierte Voice-over-IP-Telefonate mit internationalen Anbietern. Die bestehenden Möglichkeiten der Telekommunikationsüberwachung stoßen bei der Internet-Telefonie und ihrer technischen und organisatorischen Komplexität an ihre Grenzen. Die Software Skype überträgt die Sprachdaten grundsätzlich verschlüsselt.

- Frei zugängliche Möglichkeiten der Kryptierung, der Steganografie und Anonymisierung, die Verschleierung von IP-Adressen und die Verwendung von Passwörtern lassen klassische polizeiliche Ermittlungsinstrumente immer mehr ins Leere laufen. Die Dekryptierung von sichergestellten IT-Beweismitteln und Kommunikationsdaten ist nur mit erheblichem Aufwand oder überhaupt nicht möglich.
- Immer mehr werden E-Mail-Accounts genutzt, deren Daten auf ausländischen Servern abgelegt sind. Den von den Tätern in Millisekunden vollzogenen Sprung über nationale Grenzen hinweg müssen die Strafverfolgungsbehörden auf dem langwierigen monatelangen Weg der Rechtshilfe nachvollziehen.
- Schadprogramme im Internet werden zunehmend modular aufgebaut. Kleine Programme – so genannte Downloader - gewinnen an Bedeutung. Sie laden Schadprogramme nach, unterlaufen Virenschutzprogramme und vermindern so die Abwehrmöglichkeiten.

## WIE HABEN WIR IN DEN POLIZEIEN VON BUND UND LÄNDERN BISHER AUF DIESE ENTWICKLUNG REAGIERT?

Einige Beispiele:

- Seit Mitte der 1990er Jahre gibt es Dienststellen für anlassunabhängige Recherchen im Internet, im BKA die „Zentralstelle für anlassunabhängige Recherchen in Datennetzen“, kurz ZaRD genannt. Die Online-Streife sucht im Internet systematisch nach strafbaren Inhalten - deliktsübergreifend. Bund und Länder haben eine gemeinsame „Koordinierungsgruppe für anlassunabhängige Recherchen im Internet“ (KaRIn) eingerichtet.
- Das „Gemeinsame Internetzentrum“ (GIZ) als Internet-Monitoringstelle befasst sich seit dem Jahr 2007 mit dem internationalen religiös motivierten Terrorismus. Das ist gestern von Herrn Minister Dr. Schäuble ausführlich dargestellt worden. Gleiches gilt auch für die Initiative „Check the web“.
- Um unsere Möglichkeiten im Bereich der Internetüberwachung weiter auszubauen, arbeiten wir an der Entwicklung einer Software, genannt NetCrawler. Die Forschungs-Hypothese lautet, dass häufige Veränderungen extremistischer oder terroristischer Web-Sites eventuell Vorhersagen auf bevorstehende Aktivitäten ermöglichen können.
- Zusammen mit den Internet-Service-Providern sollen die Möglichkeiten des so genannten Access-Blockings genutzt werden. Auf diese Weise wollen wir den Zugriff auf kinderpornografische Angebote im Internet nachhaltig stören.
- Um die Polizeipräsenz im Internet zu erhöhen, haben einige Bundesländer so genannte Online-Wachen eingerichtet. Opfer haben auf diese Weise die Möglichkeit, Straftaten direkt im Internet - über eine entsprechende Homepage der Polizei – anzuzeigen.

Reichen diese Maßnahmen aus? Dies ist abhängig von der Frage, mit welchen **phänomenologischen Kriminalitätstrends** wir es heute im Internet zu tun haben.

Es gibt heute kaum noch einen Kriminalitätsbereich, in dem das Internet als Tatmittel keine Rolle spielt. Die Palette reicht von Betrugsdelikten, Computerkriminalität und Verbreitung von Kinderpornografie über Organisierte Kriminalität, Wirtschaftskriminalität und Wirtschaftsspionage bis hin zur Planung terroristischer Anschläge.

Für das Jahr 2006 registrierte die Polizei mehr als 165.000 Fälle mit dem **Tatmittel Internet** – im Vergleich zum Vorjahr eine Steigerung um 40 Prozent. Bei den in der Polizeilichen Kriminalstatistik (PKS) erfassten Straftaten mit dem Tatmittel Internet handelt es sich überwiegend um Betrugsdelikte (83 %). Besonders hervorzuheben ist hierbei der Warenbetrug, der allein mehr als die Hälfte aller Fälle (52 %) ausmacht.

Aber: Der Anteil der Wirtschaftskriminalität lag bei etwa 9.700 Fällen, also rund vier Prozent. Ein Blick auf die Vorjahre zeigt: Immer häufiger wird das Internet bei der Begehung von Wirtschaftsstraftaten genutzt. Die Tatzahlen haben sich seit 2004 mehr als verdreifacht.
Die in der PKS erfassten Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden - kurz bezeichnet als **IuK-Kriminalität** - bewegen sich seit 2002, was die IuK-Kriminalität im engeren Sinne betrifft, auf einem relativ stabilen, aber hohen Niveau von rund 30.000 Straftaten jährlich.

Wir gehen aber auch von einem erheblichen Dunkelfeld aus. Dafür sprechen folgende Indizien:

- Oftmals bleibt der Einbruch in den Rechner für das Opfer unentdeckt.
- Geschädigte Unternehmen sehen häufig von einer Anzeige ab, weil sie einen Imageverlust befürchten. Bemerkenswert ist: 50 % der Unternehmen in Deutschland haben immer noch keine schriftlich fixierte IT-Sicherheitstrategie.

IuK-Kriminalität ist durch eine besondere Dynamik gekennzeichnet. Die Täter passen sich äußerst schnell an. Die Ihnen allen bekannten Phishing-Mails, die zum Klicken auf einen Link auffordern, haben kaum noch Bedeutung. Phishing mit Trojanischen Pferden steigt dafür deutlich an. Mit Hilfe dieser Programme, die ohne Wissen der Besitzer auf Rechnern aktiv werden, verfügt der Angreifer über umfangreiche Kommunikations- und Steuerungsmöglichkeiten sowie eine Vielzahl von Funktionen, die sich beliebig kombinieren lassen (geschätzt für Deutschland 2006 ca. 750.000 infizierte Rechner): Trojanische Pferde können fremde Rechner vollständig kontrollieren, Daten ausspionieren, Tastatureingaben und Bildschirmausgaben aufzeichnen oder IT-Systeme sabotieren. Der Trojaner ist dann überall. Sie überwachen im Hintergrund den für Online- Überweisung im E-Banking typischen Netzverkehr.
Direkt vor der Übermittlung an den Bankrechner werden Konto-Nummer, PIN und TAN der Geschädigten abgegriffen. Mit automatisierten so genannten Man-in-the-Middle-Attacken lassen sich auch Einmalpasswörter wie iTAN ausspähen. Zusätzlich besitzen sie hoch entwickelte Tarnfunktionen und laden Updates über das Internet auf die infizierten Rechner. Trojanische Pferde werden für den Aufbau von Bot-Netzen und bei Phishing-Angriffen eingesetzt.

Schadprogramme sind heute weniger darauf ausgerichtet, direkte und bemerkbare Schäden anzurichten. Den Tätern geht es vor allem darum, Kontrolle über Rechner zu erlangen und Daten auszuspionieren. Von daher ist es das vorrangige Ziel der Programmierer von Schadprogrammen, diese auf infizierten Computern dauerhaft zu

installieren. So können Daten über einen längeren Zeitraum gesammelt werden - beispielsweise, um diese an andere Kriminelle zu verkaufen. Für Schadprogramme gibt es einen eigenen Markt im Internet.

**Wirtschaftsspionage** kann man heute bequem vom Schreibtisch aus betreiben: 2006 erhielten wir von Scotland Yard die Mitteilung über einen Hacker, der sich im Auftrag eines britischen Unternehmens in die Systeme einer norddeutschen Spedition gehackt hatte. Dort platzierte er Software, die nahezu den gesamten elektronischen Geschäftsverkehr ausspionierte und an die britische Firma weiterleitete. Ziel dieses Angriffs war die Übernahme der deutschen Spedition.

Das Internet als Tatmittel spielt auch bei der Verbreitung von **Kinderpornografie** die zentrale Rolle. Die Zahlen der PKS bewegen sich hier seit Jahren auf hohem Niveau: 2006 wurden deutlich über 7.000 Fälle mit etwa 6.000 Tatverdächtigen im Bereich Besitz und Verbreitung registriert.[1] Die Opfer werden immer jünger. Immer häufiger stoßen wir auf Bilder im Internet, auf denen Gewaltausübungen dokumentiert sind und Kleinkinder sowie Babys schwer missbraucht werden. Kinderpornografie ist ein Wachstumsmarkt, dessen Ausmaß nur schwer abzuschätzen ist. Die festgestellten Zugriffe auf inkriminierte Dateien belaufen sich im Einzelfall auf mehrere 100.000. In einem Verfahren in Deutschland haben wir über 238.000 Zugriffe auf 4.600 kinderpornografische Dateien festgestellt.

Das Internet hat insbesondere die Infrastruktur **terroristischer Netzwerke** erheblich verändert. Ursächlich dafür dürften vor allem der nach dem 11. September 2001 weltweit erhöhte Fahndungsdruck und die daraus resultierende verstärkte Konspiration der Täterseite sein. Terroristische Netzwerke nutzen das Internet für Propagandazwecke, für Aufrufe zu Spendensammlungen, zur Radikalisierung, zur Rekrutierung und zur Ausbildung neuer Unterstützer und Kämpfer ebenso wie zur Tatvorbereitung und hoch konspirativer Kommunikation.
Die so genannten Kofferbomber fanden die Anleitungen zum Bau der Bomben, die im vergangenen Jahr in zwei Regionalzügen abgelegt waren, ebenso im Internet wie die Fatwa, ein islamisches „Rechtsgutachten“, mit dem sie ihre Taten gerechtfertigt glaubten.
Auch die jungen Männer, die wir Anfang September in Oberschlehdorn festgenommen haben, nutzten das Internet intensiv für ihre Zwecke. Sie haben Informationen gesucht, auf ihren Laptops gespeichert und diese untereinander ausgetauscht. Sie suchten ungesicherte WLANs, z. B. in Wohngebieten, um sich darüber unbemerkt ins Internet einzuloggen.

Meine sehr verehrten Damen und Herren,
das Tatmittel Internet hat klassische **Viktimisierungsprozesse** erheblich verändert. Alle Besitzer eines Internetzugangs und damit 60 Prozent aller Haushalte in Deutschland sind permanent in der Gefahr, ihren Rechner mit Schadsoftware zu infizieren.
Daraus den Schluss zu ziehen, wir sollten künftig auf das Internet verzichten, ist natürlich falsch. Auf die Vorteile des Internets können und wollen wir nicht mehr verzichten. Aber gleichzeitig gilt: Beim Surfen im Netz reichen einige unbewusste Klicks oder Unaufmerksamkeiten beim Öffnen einer Mail aus und Dritte übernehmen das Kommando über den eigenen Rechner, steuern ihn sozusagen fern und missbrauchen ihn für kriminelle Zwecke – und das trotz technischer Schutzprogramme.

[1] PKS 2005: 8.200 Fälle, 6.400 Tatverdächtige – PKS 2006: 7.318 Fälle, 6.100 Tatverdächtige

Der Besitzer des Rechners wird somit nicht nur selbst zum Opfer, der Täter macht ihn auch noch zu seinem Werkzeug.
Erschwerend kommt hinzu, dass die Täter ihr Social Engeneering zunehmend professioneller betreiben: Mit immer raffinierteren Geschichten werden Anwender dazu gebracht, E-Mails zu öffnen oder auf vermeintlich legale Angebote einzugehen. Auch weil immer mehr Anwender bereit sind, private Details im Internet auf offenen Webseiten oder in Diskussionsforen preiszugeben.

Und selbst der Personenkreis, der keinen Zugang zum Internet hat, kann durch das Internet zum Opfer werden. Dies ist beispielsweise der Fall, wenn illegal erlangte Kreditkartendaten oder Bilder von sexuellen Missbrauchs- oder Gewalthandlungen ins Netz gestellt werden.
Beim Handel mit kinderpornografischem Bildmaterial wird zudem deutlich, dass die Nutzung des Internets die Intensität der Viktimisierung verschärft:

- Die weltweite Vernetzung der Täter, die damit einhergehende massenhafte Verbreitung des Bildmaterials – all dies ist mit dem früher typischen Austausch von Bildern in klandestinen Zirkeln in keiner Weise vergleichbar.
- Per Knopfdruck werden heute Missbrauchsszenen massenhaft vervielfacht und sind quasi in Echtzeit an jedem Ort der Welt verfügbar.

Für das Opfer bedeutet dies: Neben der eigentlichen Missbrauchshandlung entsteht durch die ungehinderte Verbreitung des Bildmaterials im Internet eine andauernde Phase der Viktimisierung – möglicherweise über viele Jahre hinweg – vielleicht ein Leben lang. Wer kann eine solche Belastung auf Dauer ertragen?

Meine sehr verehrten Damen und Herren,

genauso falsch ist sicherlich auch die Forderung, das Internet müsse frei von jeglichen Beschränkungen sein, der Bürger müsse Schäden als Teil des allgemeinen Lebensrisikos in Kauf nehmen. Das Internet darf kein verfolgungsfreier Raum sein! Die Polizei ist gefordert, den Schutzauftrag des Staates für alle Bürger zu erfüllen und Kriminalität zu bekämpfen – unabhängig davon, in welcher Form und an welchem Ort sie verübt wird. Dies kann und muss heute selbstverständlich auch der virtuelle Raum sein. Wir müssen sicherstellen, dass die Nutzung des Internets für jedermann möglich ist, ohne dass damit schwerwiegende Gefahren verbunden sind.
Wer diesen Anspruch aufgibt, weil er meint, dies sei der Preis der Freiheit, denn hundertprozentige Sicherheit könne es ohnehin nicht geben, der kündigt das Sicherheitsversprechen des Staates gegenüber seinen Bürgern auf – zugleich eine wesentliche Rechtfertigung des staatlichen Gewaltmonopols.

Der Staat ist von Verfassungs wegen verpflichtet, die Sicherheit der Bevölkerung zu gewährleisten. Das Bundesverfassungsgericht hat betont: Es besteht ein unabweisbares Bedürfnis für eine wirksame Strafverfolgung und Verbrechensbekämpfung. Es besteht ein öffentliches Interesse an einer möglichst vollständigen Wahrheitsfindung im Strafverfahren - natürlich nicht um jeden Preis. Die wirksame Aufklärung gerade schwerer Straftaten ist wesentlicher Auftrag eines rechtsstaatlichen Gemeinwesens, so das Bundesverfassungsgericht.

Im Hinblick auf den internationalen Terrorismus verkennen die Kritiker auch die innere Logik des Terrorismus. Terroristen wollen viele Opfer. Das individuelle Opfer interessiert im Grunde nicht, es ist nur Mittel zum Zweck. Die Ziele sind, massenhaft

Angst und Schrecken zu verbreiten und dadurch Druck auf die Politik, auf den Staat und dessen Entscheidungsträger auszuüben. Der Staat soll terroristischer Erpressung nachgeben.

Eine solche „Preis der Freiheit - Argumentation“ ist aber auch ethisch fragwürdig und bei näherer Betrachtung zynisch. Sie kann den Opfern von Straftaten keine akzeptable Perspektive vermitteln, außer auf ein „Hilf Dir selbst!“ zu verweisen, die in letzter Konsequenz zum Recht des Stärkeren führt. Vor allem sollte es immer auch um den oder die Anderen gehen, die es trifft und nicht nur um die eigene Person. Eine ethische Begründung bleiben diese Vertreter der „Preis der Freiheit - Argumentation“ bisher schuldig.

## WIE MÜSSEN SICH DIE SICHERHEITSBEHÖRDEN IN DIESER DIGITALEN WELT AUFSTELLEN?

Im Kern geht es darum, den technologischen Vorsprung der Gefährder- und Täterseite so schnell wie möglich aufzuholen.
Dabei muss der rasant voranschreitende technologische Wandel bei der Suche nach Lösungen bereits heute mit vorausgedacht werden. Der Polizei neu zur Verfügung gestellte Instrumente dürfen am Ende des Gesetzgebungsverfahrens nicht bereits veraltet sein - wir brauchen flexible rechtliche Rahmenbedingungen, also technikoffene Lösungen.

Bereits in einer möglichst frühen Phase terroristischer Planung müssen wir mit den verdeckten Instrumentarien der Strafverfolgung und Gefahrenabwehr ansetzen, um das gesamte Netzwerk aufdecken und um im Ergebnis verheerende Anschläge verhindern zu können. Ermittlungstaktisch fatal wäre es, frühzeitig offene Ermittlungsmaßnahmen wie Wohnungsdurchsuchungen und Beschlagnahmen durchzuführen. Dadurch würde das Netzwerk gewarnt und die Anschlagsplanungen – ohne unser Wissen und vor allem ohne Interventionschance – verändert und weitergeführt werden. Die Festnahmen von Oberschlehdorn im September sind dafür ein eindrücklicher Beweis.

Polizeiliches Handeln ist einsatztaktisch nicht dadurch geprägt, in jeder Phase der Ermittlungen alle zur Verfügung stehenden Überwachungsmaßnahmen anzuwenden. Im Übrigen lässt das Prinzip der Verhältnismäßigkeit ein solches Vorgehen auch nicht zu.
Wir greifen auf Maßnahmen zurück, die zweckgeeignet und mit Blick auf die jeweils aktuelle Gefahrenlage auch angemessen und zielgerichtet sind.
Das bedeutet, dass wir eine breite Auswahl an Instrumenten in unserem Instrumentenkasten benötigen, die von der Schwere und Sozialschädlichkeit eines Delikts genauso wie vom speziellen Modus Operandi der Täterseite abhängig sind. Das von Kritikern beliebte Aneinanderreihen aller möglichen Befugnisse der Sicherheitsbehörden erklärt nicht den spezifischen Sinn der einzelnen Maßnahme. Es vernebelt bewusst und soll Missbrauchsängste entfachen.
Bewährte Methoden wie der Einsatz von Verdeckten Ermittlern und Vertrauenspersonen, die klassische Telefonüberwachung oder die akustische Wohnraumüberwachung müssen sich mit neuen Überwachungsmöglichkeiten sinnvoll ergänzen.

Meine sehr verehrten Damen und Herren,
die aktuelle Diskussion über neue Eingriffsbefugnisse muss sachlicher geführt werden. Die Debatte über den möglichen Missbrauch von Befugnissen, die den allgegenwärtigen Überwachungsstaat suggeriert, ist eine Angstdebatte. Das beste Beispiel ist die akustische Wohnraumüberwachung. Verfassungsgemäß und sehr behutsam wird sie eingesetzt. Keine der Befürchtungen der Kritiker hat sich erfüllt. Bewusst werden heute die aktuellen Gefahren der terroristischen Bedrohung ausgeblendet und klein geredet. Der Diskurs verharrt so im Abstrakten und Hypothetischen. Tatsächlich sind die Sicherheitsbehörden mit Risiken konfrontiert, die eigentlich nicht zu verantworten sind. Ich nehme diejenigen ernst, die sich Sorgen machen um die freiheitliche Grundrechtsausübung in unserem Staat. Lassen Sie uns aber über Kontrollmechanismen diskutieren, statt Misstrauen gegen die Sicherheitsbehörden zu verbreiten. Gefährdungen zu ignorieren, die offenkundig sind, macht mich zumindest sehr nachdenklich.
Das **rechtliche Instrumentarium** ist daher anzupassen. In der Internetwelt des 21. Jahrhunderts sehe ich dazu keine realistische Alternative.

## Zur Vorratsdatenspeicherung

Um frühzeitig Ansatzpunkte für Überwachungsmöglichkeiten zu gewinnen und Angehörige krimineller Netzwerke identifizieren bzw. die Strukturen solcher Netzwerke überhaupt erhellen zu können, benötigen wir eine Speicherung von Telekommunikationsverbindungsdaten und IP-Adressen durch die **Provider**.
Ohne IP-Adressen ist z. B. die Bekämpfung von Kinderpornografie im Internet nicht möglich. Die Inhalte der Kommunikation werden nicht gespeichert. Die Identifizierungspflicht der IP-Inhaber steht im Vordergrund. Diesem Erfordernis hat der Gesetzgeber mit der neuen Regelung zur Vorratsdatenspeicherung Rechnung getragen und die Dauer der Speicherung auf sechs Monate festgelegt. Dabei bleiben wir an der untersten Grenze dessen, was die europäische Rahmenrichtlinie zuließ.
Und was auch wichtig ist: Keine Sicherheitsbehörde speichert diese Verbindungsdaten auf Vorrat. Wir haben nur in gesetzlich geregelten Fällen, auf Grund eines richterlichen Beschlusses Zugriff.

## Zur Online-Durchsuchung

Verschlüsselung darf in einem Rechtsstaat nicht vor Strafverfolgung schützen. Verfolgungsfreie Räume im Internet sind nicht hinnehmbar.
Die Online-Durchsuchung bietet die Möglichkeit, auf die relevanten Daten verdeckt, frühzeitig und vor allem gezielt zugreifen zu können, bevor diese verschlüsselt oder unauffindbar im Internet abgelegt werden. Selbstverständlich mit richterlichem Beschluss.
Es werden keine „Hackertools“ oder „Trojaner“ zum Einsatz kommen, wie sie von Kriminellen genutzt werden. Wir benötigen keine back doors kommerzieller Programme. Wir entwickeln Software als Unikate, die auch auf mögliche Risiken für Betroffene und Unbeteiligte hinreichend überprüft werden. Diese Software ist so ausgestaltet, dass auf den Zielsystemen keine Daten manipuliert werden. Der gesamte Einsatz wird umfangreich forensisch dokumentiert und ist vor allem durch die Gerichte immer nachvollziehbar.

Bei kryptiertem E-Mail-Verkehr bieten sich als Zugriffspunkt zur Überwachung lediglich die jeweils bekannten Endgeräte an. Die Online-Durchsuchung gibt uns in diesen Fällen die Chance, bereits abgelegte E-Mails oder Dateianhänge aufzufinden, die möglicherweise Hinweise auf den Absender bzw. Empfänger beinhalten.
Ein zunehmendes Problem ist die Nutzung von E-Mail-Accounts, deren Daten auf ausländischen Servern abgelegt sind. Eine Live-Überwachung der Kommunikation ist in solchen Fällen entweder über ein im Ausland geführtes so genanntes Spiegelverfahren oder durch Einrichtung eines Joint Investigation Teams theoretisch möglich.
Gelingt das nicht, können wir nur im Wege der klassischen Rechtshilfe mit erheblichem zeitlichem Verzug rückwirkend Daten erlangen. Dies hat in Gemengelagen für die Gefahrenabwehr fatale Folgen, da wir die für eine Anschlagsverhinderung notwendigen Informationen eventuell viel zu spät erhalten.

Kritiker meinen, dass wir mit der Online-Durchsuchung nur die so genannten DAUs - gemeint ist der Dümmste anzunehmende User - erwischen. Natürlich kann jede einzelne Ermittlungsmaßnahme durch Gegenstrategien ausgehebelt werden. Das ist bei allen klassischen Ermittlungsmaßnahmen der Fall. Sollten wir einen Anschlag mit Toten und Verletzten in Deutschland durch die Festnahme eines so genannten DAU verhindern, wären sicherlich auch die Kritiker sehr erleichtert. Letztlich hängt es vom gesamten kriminaltaktischen Konzept ab, ob Beweise erbracht und Gefahren abgewehrt werden können. Die kriminalpolizeiliche Praxis belegt, dass Straftäter – unabhängig von ihrer Intelligenz oder Erfahrung – ihr kriminelles Handeln nicht in der Weise beherrschen, dass sie Ermittlungserfolge gänzlich verhindern können. Insbesondere nicht in Netzwerken, in denen eine Vielzahl von Personen – jeweils mit unterschiedlichen Aufgaben beauftragt - kommuniziert. Das perfekte Verbrechen gibt es nicht.

Darüber hinaus wird der Eindruck vermittelt, jeder könnte Betroffener einer Online-Durchsuchung werden. Mit dem Instrument der Online-Durchsuchung ist eine flächendeckende oder auch Schleppnetzfahndung weder beabsichtigt noch möglich. Auch ist der Aufwand viel zu groß. Es geht um Schwerstkriminalität – um Einzelfälle.

Zum Kernbereichsschutz: Der Kernbereich privater Lebensgestaltung muss gewahrt bleiben! Nicht jeder private Inhalt gehört zum Kernbereich und ist unantastbar. Es ist in jedem Einzelfall zu prüfen, ob der Inhalt dem absolut zu schützenden Kernbereich unterliegt oder nicht. Der Kernbereich ist nach ständiger Rechtsprechung des Bundesverfassungsgerichts dann nicht verletzt und die Information der staatlichen Kenntnisnahme damit zugänglich und für das Verfahren verwertbar, wenn die erlangte Information unmittelbaren Bezug zu einer Straftat hat. Auch im Kernbereich der privaten Lebensgestaltung dürfen keine Straftaten begangen werden!

## Zur Quellen-TKÜ

Die Quellen-TKÜ hat für die Sicherheitsbehörden eine sehr große Bedeutung. Etwa 70 % der Aufklärungserfolge der Organisierten Kriminalität in Deutschland haben ihren Ursprung in der heutigen Telekommunikationsüberwachung (TKÜ). Bei der Quellen-TKÜ handelt es sich um eine besondere Form der konventionellen TKÜ. Sie ermöglicht die Überwachung verschlüsselter Internet-Telefonie. Die Quellen-TKÜ ist zwar technisch vergleichbar mit der Online-Durchsuchung, verfolgt jedoch einen gänzlich anderen Zweck.

Hier wird die laufende Kommunikation vor der Verschlüsselung bzw. nach der Entschlüsselung abgegriffen. Eine Durchsuchung sonstiger, z. B. auf der Festplatte gespeicherter Daten findet bei der Quellen-TKÜ, nicht statt.

Die Quellen-TKÜ ist von daher keine Alternative zur Online-Durchsuchung. Die filigrane Rabulistik von der so genannten geronnenen Kommunikation halte ich in diesem Zusammenhang für nicht praxistauglich.

## Zum Thema Massendaten

Meine sehr geehrten Damen und Herren,
neben dem Problem kryptierter Daten stehen wir vor einer weiteren Herausforderung: Die weit verbreitete Nutzung von Massenspeichern führt dazu, dass mehr Datenmaterial gesichert wird, als mit herkömmlichen Methoden kriminalistisch ausgewertet werden kann. Dieses Problem der Massendaten stellt sich im Übrigen auch bei der Überwachung der Kommunikation (TKÜ). Dies ist teilweise auch eine Folge fehlender Eingriffsbefugnisse. Mit der Online-Durchsuchung könnten wir viel früher relevante Dateien erkennen. Berufskritiker ziehen jedoch schon weitergehende Schlüsse: Weil nicht sofort alles ausgewertet werden könne, ergebe die gesamte Maßnahme nach deren Auffassung keinen Sinn.

Um Massendaten auszuwerten, setzen wir ein spezielles Auswertetool ein. Dessen Funktionalitäten sollen durch Fremdsprachenerkennung und Metadatenextraktion erweitert werden. Auch die Integration von Text-Mining-Algorithmen ist geplant, um dem polizeilichen Sachbearbeiter intelligente Suchanfragen an das System zu ermöglichen. Daran erkennen Sie, welch hohe Anforderungen an die polizeiliche Aus- und Fortbildung zu stellen sind.

Meine sehr verehrten Damen und Herren,
angesichts der aktuellen Herausforderungen ist offensichtlich, dass die Polizei für eine effektive und effiziente Erfüllung ihres gesetzlichen Auftrags über eine hervorragende **IT-Infrastruktur** verfügen muss.

Um dies zu gewährleisten, müssen wir auch **perspektivisch forschen**. Die Polizei muss Chancen und Risiken moderner Technologien für die Kriminalitätsbekämpfung rechtzeitig abschätzen können. Das BKA entwickelt derzeit eine Methode des **Technologiemonitorings**. Forschung, Entwicklung und Vermarktung neuer Technologien werden kontinuierlich beobachtet. Auf diese Weise werden diejenigen Technikbereiche identifiziert, aus denen mit hoher Wahrscheinlichkeit Ermittlungshemmnisse und neue Kriminalitätsformen, aber auch möglicherweise neue Ansätze der Kriminalitätsbekämpfung erwachsen werden.

Eine enge Kooperation auf Bund-Länder-Ebene soll helfen, insbesondere die prognostizierten technischen Schwierigkeiten und Kapazitätsprobleme bei der TKÜ gemeinsam zu überwinden. Zur Bündelung unserer Ressourcen sollten auf Bundesebene neben einem **Servicezentrum**, das insbesondere den technischen Betrieb entsprechender Anlagen und deren Service sicherstellt, auch die für die Anwenderseite wichtigen Fragen der Strategie, der Methodenentwicklung und Koordination organisatorisch in einem **Kompetenz-Center** zusammengeführt werden. Bund und Länder müssen diese Zukunftsaufgabe gemeinsam bewältigen.

Meine sehr verehrten Damen und Herren,
ich fasse abschließend kurz zusammen:

Der rasante technische Wandel verändert Tat- und Tätertypologien grundlegend.

1. Klassische kriminalgeographische Räume werden durch den virtuellen Raum entgrenzt. Die Dezentralität des Internets befördert die Dezentralität von Netzwerken des Terrorismus und der Organisierten Kriminalität. Aber auch der Aktionsraum von Einzeltätern ist per Mausklick weltumspannend.
2. Verschlüsselung und Anonymisierung schaffen verfolgungsfreie Räume mit fatalen Folgen für die Innere Sicherheit, sowohl für die Strafverfolgung als auch für die Gefahrenabwehr.
3. Die Ungleichzeitigkeiten von Technik und Recht müssen beseitigt werden. Der Staat darf sich nicht blind, taub und handlungsunfähig machen.

Für die Sicherheitsbehörden von Bund und Ländern heißt das: Wir brauchen eine **Kriminalistik der digitalen Welt**.

Das heißt:

- Wir brauchen technikoffene und damit flexible rechtliche Regelungen zur Strafverfolgung und Gefahrenabwehr.
- Wir brauchen die Online-Durchsuchung als wirkungsvolle Maßnahme zur Aufhellung *gespeicherter* Daten und Informationen.
- Wir brauchen die Quellen-TKÜ als unverzichtbare Maßnahme zur Kommunikationsüberwachung insbesondere im Bereich der Organisierten Kriminalität und des Terrorismus.
- Wir benötigen die entsprechende technische, sehr spezialisierte Ausstattung und entsprechende Mitarbeiter, um die Auswertung von Massendaten bewältigen zu können. Zur Bündelung knapper Ressourcen führt kein Weg an der Bildung von Kompetenz-Centern in Deutschland vorbei.

Das Bundeskriminalamt und die Polizeien des Bundes und der Länder stehen für die Bewahrung rechtsstaatlicher Freiheiten und für einen offenen und fairen Dialog auf der Basis unserer Lage- und Gefährdungserkenntnisse. Zu einem solch fairen Dialog, der ein kritischer Diskurs sein kann, fordere ich unsere Kritiker auf.